CENTER FOR HEALTH INFORMATION & ANALYSIS
ADDENDUM TO DATA USE AGREEMENT
FOR RECIPIENTS OF MEDICARE DATA

This Addendum supplements the Data Use Agreement ("DUA") between the Center for Health Information and Analysis ("CHIA") and _____ ("Data Recipient"), effective as of the date of execution below. To the extent that this Addendum is inconsistent with any terms in the DUA, this Addendum modifies and overrides the DUA.

This Addendum addresses the conditions under which CHIA will disclose and the Data Recipient will obtain, use, reuse and disclose data file(s) belonging to the Centers for Medicare and Medicaid Services ("CMS Data") that contain direct individual identifiers or elements that can be used in concert with other information to identify individuals.

A-1. Ownership of the Data: The Data Recipient acknowledges that CMS retains all ownership rights to the data file(s) referred to in this Agreement, and that the Data Recipient does not obtain any right, title, or interest in any CMS Data provided by CHIA.

A-2. Use and Reuse of the Data: The Data Recipient agrees not to disclose, use, or reuse CMS Data except as except as specified in the Data Recipient's DUA with CHIA, as modified by this Addendum, or except as CHIA shall authorize in writing or as otherwise required by law.

A-3. Minimum Data Necessary: The Data Recipient affirms that the requested CMS Data is the minimum necessary to achieve the purposes stated in the data request attached to the Data Recipient's DUA with CHIA as Exhibit A. The Data Recipient agrees that within the Data Recipient organization, and the organizations of its agents, access to the data covered by this Addendum shall be limited to the minimum amount of data and minimum number of individuals necessary to achieve the purposes stated in the data request attached to the Data Recipient's DUA with CHIA as Exhibit A.

A-4. Data Linking: As long as the resulting files are only used for the research purposes delineated in the data request attached to the Data Recipient's DUA with CHIA as Exhibit A, nothing in the DUA prohibits the Data Recipient from linking records included in CMS Data file(s) to other sources of individually identifiable information.

A-5. Data Storage: The Data Recipient agrees to ensure that each site at which CMS Data is stored includes the appropriate administrative, technical, and physical safeguards to protect the confidentiality of, and to prevent the unauthorized use or access to the data. The safeguards shall provide a level and scope of security that is not less than the level and scope of security requirements established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems (http://www.whitehouse.gov/omb/circulars/a130/a130.html) as well as Federal Information Processing Standard 200 entitled "Minimum Security Requirements for Federal Information and Information Systems" (http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf); and, Special Publication 800-53 "Recommended Security Controls for Federal Information Systems" (http://csrc.nist.gov/ publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf). The Data Recipient acknowledges that the use of unsecured telecommunications, including the Internet, to

transmit individually identifiable, bidder identifiable, or deducible information derived from CMS data file(s) is prohibited. The Data Recipient agrees to keep a record of all sites where CMS Data or any derivative data are stored.

A-6. Disclosure of Findings: The Data Recipient agrees not to disclose direct findings, listings, or information derived from the CMS Data file(s), with or without direct identifiers, if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce an individual's identity. Examples of such data elements include, but are not limited to geographic location, age if > 89, sex, diagnosis and procedure, admission/discharge date(s), or date of death. The Data Recipient agrees that any use of CMS data in the creation of any document (manuscript, table, chart, study, report, etc.) must adhere to CMS's current cell size suppression policy. **This policy stipulates that no cell (e.g. admittances, discharges, patients, services) 10 or less may be displayed.** Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell 10 or less. The Data Recipient also agrees not to disclose, with or without direct physician identifiers, direct findings, listings, or information derived from CMS data file(s) if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce a physician's total Medicare reimbursements.

A-7. Public Reporting: The Data Recipient acknowledges that additional requirements, including, but not limited to 42 CFR Part 401, may govern its ability to engage in public reporting regarding the performance of health care providers and suppliers using CMS Data. It is the sole responsibility of the Data Recipient to ensure that all applicable state and federal requirements are met prior to engaging in public reporting of any findings, listings, or information derived in whole or in part from CMS Data.

A-8. Breach Notification and Corrective Action: The Data Recipient agrees to immediately report any breach of personally identifiable information to CHIA, as provided in the Data Recipient's DUA with CHIA. The Data Recipient agrees that in the event CHIA determines or has a reasonable belief that the Data Recipient has made or may have made a use, reuse or disclosure of the aforesaid file(s) that is not authorized by this agreement or another written authorization, CHIA, at its sole discretion, may require the Data Recipient to: (a) promptly investigate and report to CHIA the Data Recipient's determinations regarding any alleged or actual unauthorized use, reuse or disclosure; (b) promptly resolve any problems identified by the investigation; (c) if requested by CHIA, submit a formal response to an allegation of unauthorized use, reuse or disclosure; (d) if requested by CHIA, submit a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures; and (e) if requested by CHIA, return CMS Data files to CHIA or destroy the CMS Data files it received from CHIA under this agreement. Major violations of this agreement may result in the termination of the Data Recipients' DUA with CHIA. The Data Recipient agrees to abide by CHIA's findings as to whether a violation is minor or major.

A-9. Return or Destruction of the Data: The Data Recipient agrees to return or destroy the CMS data files and any derivative data, and to send written certification of the destruction of CMS data files to CHIA, within 30 days: 1) of the completion of the research described in the data request attached to the Data Recipient's DUA with CHIA as Exhibit A; or 2) of the termination, for any reason, of CHIA's DUA with CMS or the Data Recipient's DUA with CHIA. The Data Recipient must complete a certificate of destruction to cover all sites where CMS data file(s) were physically moved, transmitted, or disclosed.

A-10. Inspections: The Data Recipient agrees to grant access to the CMS Data in its possession to the authorized representatives of CHIA, CMS, or the U.S. Department of Health and Human Services Office of the Inspector General for the purpose of inspecting to confirm compliance with the terms of this agreement and/or CHIA's compliance with the terms of CHIA's DUA with CMS.

A-11. Acknowledgment of Criminal Penalties: The Data Recipient hereby acknowledges that criminal penalties under §1106(a) of the Social Security Act (42 U.S.C. § 1306(a)), including a fine not exceeding $10,000 or imprisonment not exceeding 5 years, or both, may apply to disclosures of information that are covered by § 1106 and that are not authorized by regulation or by Federal law. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. § 552a(i)(3)) may apply if it is determined that the Data Recipient, or any individual employed or affiliated therewith, knowingly and willfully obtained the file(s) under false pretenses. Any person found to have violated section (i)(3) of the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000. Finally, the Data Recipient acknowledges that criminal penalties may be imposed under 18 U.S.C. § 641 if it is determined that the Data Recipient, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s), or received the file(s) knowing that they were stolen or converted. Under such circumstances, they shall be fined under Title 18 or imprisoned not more than 10 years, or both; but if the value of such property does not exceed the sum of $1,000, they shall be fined under Title 18 or imprisoned not more than 1 year, or both.

A-12. By signing this Addendum, the Data Recipient agrees to abide by all provisions set out herein acknowledges having received notice of potential criminal or administrative penalties for violation of the terms of the Addendum.

A-13. On behalf of the Data Recipient, the undersigned individual hereby attests that he or she is authorized to legally bind the Data Recipient to the terms this Addendum and agrees to all the terms specified herein.

For _____:
Data Recipient Organization

_____ _____
Authorized Signature Date

Print Name:_____

Title:_____

Organization:_____

Address:_____

Telephone:_____ E-Mail:_____